

**External Authentication with F5 FirePass[®] SSL VPN
appliance**

**Authenticating Users Using SecurAccess Server by
SecurEnvoy**

Contact information		
SecurEnvoy	www.securenvoy.com	0845 2600010
	1210 Parkview Arlington Business Park Theale Reading RG7 4TY	
Phil Underwood	Punderwood@securenvoy.com	

F5 FirePass® SSL VPN appliance Integration Guide

This document describes how to integrate a F5 FirePass® SSL VPN appliance with SecurEnvoy two-factor Authentication solution called 'SecurAccess'.

F5 FirePass® SSL VPN appliance provides - Secure Remote Access to the internal corporate network.

SecurAccess provides two-factor, strong authentication for remote Access solutions (such as F5 FirePass®), without the complication of deploying hardware tokens or smartcards.

Two-Factor authentication is provided by the use of (your PIN and your Phone to receive the one time passcode)

SecurAccess is designed as an easy to deploy and use technology. It integrates directly into Microsoft's Active Directory and negates the need for additional User Security databases. SecurAccess consists of two core elements: a Radius Server and Authentication server. The Authentication server is directly integrated with LDAP or Active Directory in real time.

SecurEnvoy Security Server can be configured in such a way that it can use the existing Microsoft password. Utilising the Windows password as the PIN, allows the User to enter their UserID, Windows password and One Time Passcode received upon their mobile phone. This authentication request is passed via the Radius protocol to the SecurEnvoy Radius server where it carries out a Two-Factor authentication. SecurEnvoy utilises a web GUI for configuration, as does the F5 FirePass® SSL VPN appliance. All notes within this integration guide refer to this type of approach.

The equipment used for the integration process is listed below:

F5

F5 FirePass® SSL VPN appliance v5.4.1

SecurEnvoy

Windows 2003 server SP1

IIS installed with SSL certificate (required for remote administration)

Active Directory installed or connection to Active Directory via LDAP protocol.

SecurAccess software release v3.01.0200

Index

1.0 Pre Requisites	3
2.0 Configuration of SecurEnvoy	5
3.0 Test Logon.....	5
4.0 Single Sign On	6

1.0 Pre Requisites

It is assumed that the F5 FirePass® SSL VPN appliance has been installed and basic configuration carried out.

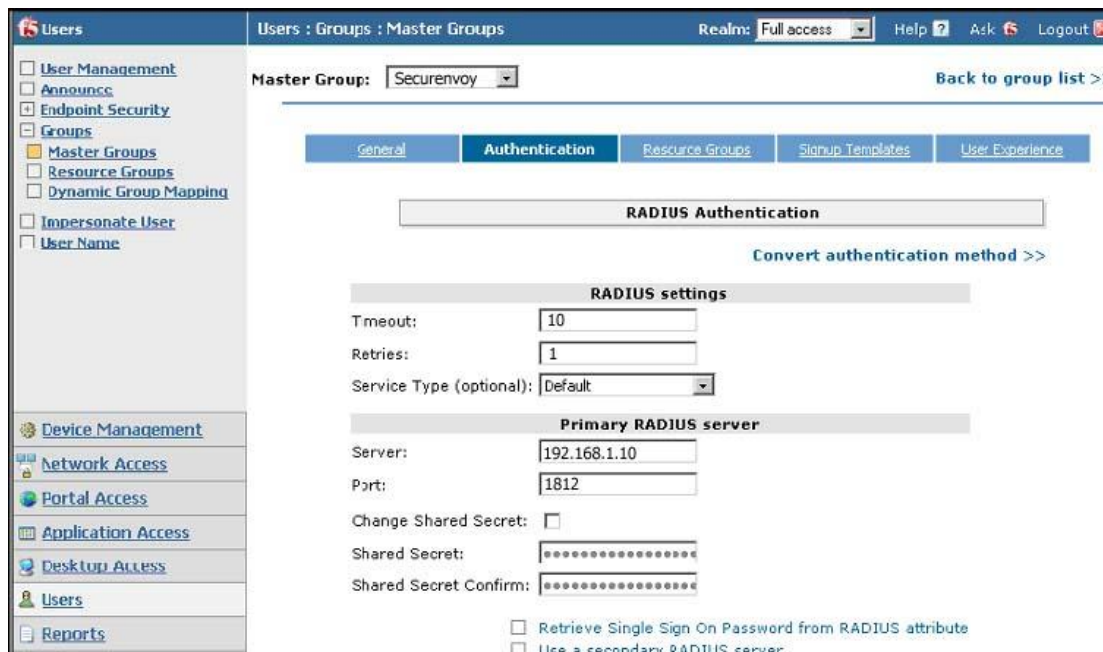
Securenvoy Security Server has been installed with the Radius service and has a suitable account that has read and write privileges to the Active Directory, if firewalls are between the SecurEnvoy Security server, Active Directory servers, and the F5 FirePass® SSL VPN appliance(s), additional open ports will be required.

NOTE: *Add radius profiles for each F5 FirePass® SSL VPN appliance that requires Two-Factor Authentication.*

1.1 Configuration of F5 FirePass® SSL VPN appliance

To enable a SecurEnvoy Two-Factor authentication logon to the F5 FirePass® SSL VPN appliance, login to the administration interface.

See diagrams below



The screenshot shows the SecurEnvoy administration interface. The left sidebar contains a navigation menu with options like User Management, Groups, and Reports. The main content area is titled "Users : Groups : Master Groups" and shows the configuration for a "Master Group" named "Secureenvoy". The "Authentication" tab is selected, displaying "RADIUS Authentication" settings. The "RADIUS settings" section includes fields for Timeout (10), Retries (1), and Service Type (Default). The "Primary RADIUS server" section includes fields for Server (192.168.1.10), Port (1812), and Shared Secret. There are also checkboxes for "Retrieve Single Sign On Password from RADIUS attribute" and "Use a secondary RADIUS server".

Navigate to "Users", "Groups", "Master Groups" and then select Create New Group button".

The Create New Group screen appears. Enter a name for this group.

Under "Users" in "Group List", select the setting for this integration, this guide uses "External".

Navigate to the authentication method list and select "Radius".

The "Copy settings from list" leave this at the "Do not copy option".

Select the "Create" button, the Master Group configuration appears.

Within the Mater Group configuration page, select the "Authentication" tab.

Enter details for "Primary Radius Server" , it is recommended for SecurEnvoy that a timeout value is set to 10 seconds or above and a retry limit of 1 is used.

Enter details for the IP address and pre-shared secret for the SecurEnvoy server.

Finally set the port information to 1812. (This is the default port on SecurEnvoy).

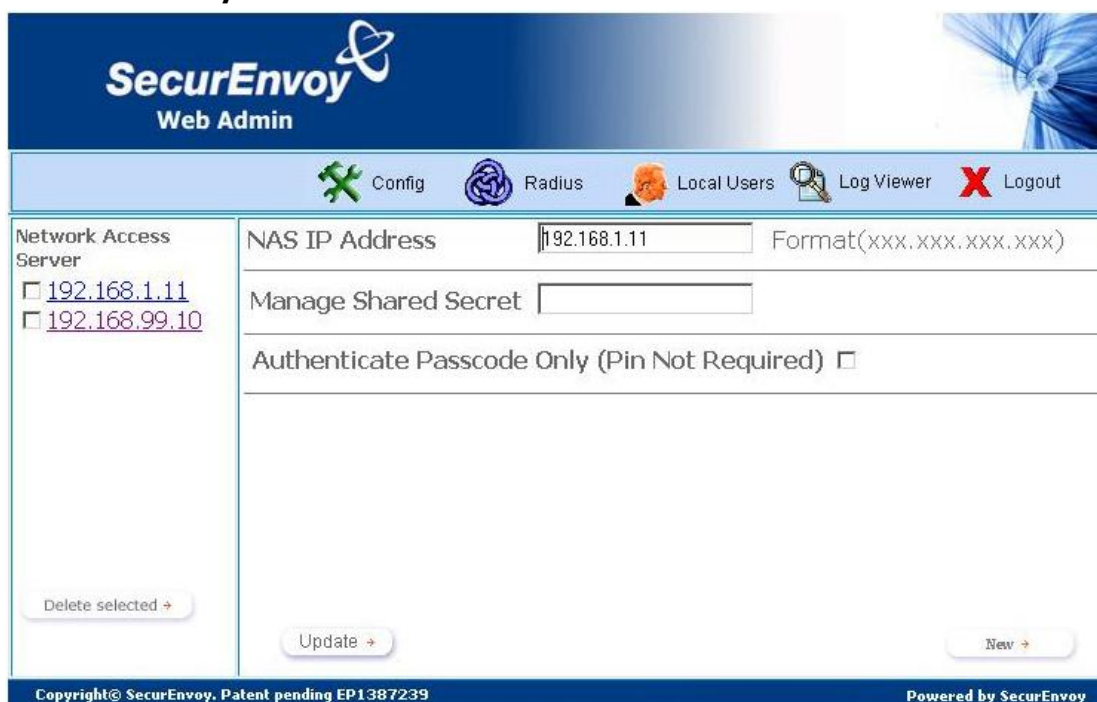
2.0 Configuration of SecurEnvoy

To help facilitate an easy to use environment, SecurEnvoy can be set up to use the existing Windows password as the PIN component. SecurEnvoy supplies the second factor of authentication, which is the dynamic one time passcode (OTP) which is sent to the user's mobile phone.

Launch the SecurEnvoy admin interface, by executing the Local Security Server Administration link on the SecurEnvoy Security Server.

Click the **"Radius"** Button

Enter IP address and Shared secret for each F5 FirePass® SSL VPN appliance that wishes to use **SecurEnvoy** Two-Factor authentication.



The screenshot shows the SecurEnvoy Web Admin interface. The top navigation bar includes 'Config', 'Radius', 'Local Users', 'Log Viewer', and 'Logout'. The main content area is titled 'Network Access Server' and contains a table with the following data:

NAS IP Address	Format(xxx.xxx.xxx.xxx)
<input type="checkbox"/> 192.168.1.11	
<input type="checkbox"/> 192.168.99.10	

Below the table, there is a 'Manage Shared Secret' field and an 'Authenticate Passcode Only (Pin Not Required)' checkbox. At the bottom of the page, there are 'Delete selected', 'Update', and 'New' buttons.

Click **"Update"** to confirm settings.

Click **"Logout"** when finished. This will log out of the Administrative session.

3.0 Test Logon

Browse to the web location of the F5 FirePass® SSL appliance

Two input dialogue boxes will be displayed.

User will enter: UserID in the User name box

Domain password in password box appended with the Passcode (via SMS)

Click logon to complete the process.

Once authenticated a new SMS passcode will be sent to the user's mobile phone, ready for the next authentication.

4.0 Single Sign On

A feature patch is available from SecurEnvoy support on request that sends the users Microsoft password back to the F5 appliance via Radius Attribute 25